IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

AMERICAN CIVIL LIBERTIES UNION, et al., Plaintiffs, v. CLEARVIEW AI, INC., a Delaware corporation, Defendant.	)	No. 2020 CH 04353 Hon. Pamela Meyerson

DEFENDANT'S REPLY MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

As set forth in Clearview's Memorandum of Law in Support of Its Motion to Dismiss ("Opening Brief"), besides being mooted by Clearview's voluntary business changes, Plaintiffs' Complaint fails, and should be dismissed pursuant to 735 ILCS 5/2-619(1) and 735 ILCS 5/2-615. Plaintiffs' response does not overcome this showing.

First, Plaintiffs point to certain Illinois contacts of Clearview to purportedly support the exercise of personal jurisdiction here. However, each alleged contact is irrelevant because it is unrelated to Plaintiffs' alleged harm. Plaintiffs do not allege that Clearview collected their biometric data from Illinois, that the collection targeted Illinois residents, or that Plaintiffs' members ever interacted with Clearview in Illinois or otherwise. Instead, Plaintiffs attempt to establish jurisdiction based on Clearview's alleged contacts with third parties in Illinois, and which occurred after Clearview had already allegedly harmed Plaintiffs' members. Those contacts cannot support specific jurisdiction for Plaintiffs' claim.

Second, Plaintiffs attempt to apply BIPA to Clearview's out-of-state activity in violation of Illinois's extraterritoriality doctrine and the U.S. Constitution's dormant Commerce Clause. Plaintiffs concede that BIPA cannot be applied extraterritorially, and so instead, Plaintiffs argue that the issue of extraterritoriality is premature. The cases cited by Plaintiffs in support for that proposition, however, are inapt. Each case turns on the fact that the Illinois-based plaintiffs in those cases had accounts with the defendants—and thus the defendants *knew* the source of the data when they were uploaded to defendants' platforms. There are no such allegations here. Plaintiffs do not and cannot allege that a majority of circumstances relevant to their claims happened in Illinois. As a result, the Complaint can—and should be—dismissed at this stage.

Relatedly, Plaintiffs cast aside Clearview's dormant Commerce Clause argument, claiming that Clearview need only "comply[] with Illinois law in Illinois and New York law in New York." Opp'n Br. at 13. Yet Plaintiffs' own allegations recognize that impossibility. Compl. ¶ 49. As a result, to be compliant with BIPA, Clearview would either need to (i) comply with BIPA with respect to all photos on the Internet or (ii) not collect any photographs on the Internet. This is the precise burden on interstate commerce that the dormant Commerce Clause is designed to avoid.

Third, Plaintiffs' claims are barred by the First Amendment, which protects "the creation and dissemination of information." That was the determination of the United States Supreme Court in *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 570 (2011). And that is precisely what Clearview does. When Clearview attempts to compare the vast amount of photographs it has collected from the public Internet—photos repeatedly held to give those photographed no reasonable expectation of privacy—with those provided to it by its law enforcement clients, it falls squarely within that protective orbit. And when Plaintiffs claim that Clearview should be enjoined from creating "faceprints" that are used by its search engines to efficiently distinguish one face from another in a publicly-available photo, unless the photographed person consents, they are seeking nothing less than the destruction of Clearview for exercising its First Amendment rights. Plaintiffs cannot satisfy any level of First Amendment scrutiny, whether it is strict scrutiny (which Clearview urges the court to apply) or intermediate scrutiny (which Plaintiffs and their *amici* urge the court to apply). There is, in short, no way the commands of the First Amendment can be met, other than to rule in Clearview's favor.

Fourth, Plaintiffs disregard the plain language of BIPA, which expressly excludes "photographs" and "information derived from" photographs. 740 ILCS 14/10. Plaintiffs argue that BIPA's definition of "biometric identifier" "says nothing about *how* these identifiers are

collected." Opp'n Br. at 24. However, BIPA's requirement of informed consent confirms the legislature's intent: the collection must be in-person, rather than from photographs. Otherwise, it would be impossible to comply with BIPA based on images obtained from public sources.

For these reasons and those in our Opening Brief, the Complaint should be dismissed.

ARGUMENT

I. Clearview Is Not Subject to Jurisdiction in Illinois

Plaintiffs do not allege that their "cause of action arises" out of the "very activity" that allegedly connects Clearview to Illinois. Opening Br. at 7 (quoting *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 780 (1984)). The Complaint should therefore be dismissed under 735 ILCS 5/2-619(1) for lack of personal jurisdiction. *See* Opening Br. at 6-10.[1]

In opposition, Plaintiffs argue that jurisdiction is appropriate because Clearview allegedly (1) licensed its search engine to Illinois entities; (2) collected Illinoisans' biometric identifiers; and (3) advertised its search engine to people in Illinois.[2] Opp'n Br. at 5, 6, 8. But none of those acts are part of the "episode-in-suit" because none give rise to or relate to the Plaintiffs' alleged harm, and indeed, none of those alleged acts involved Plaintiffs or their members. Plaintiffs allege that their members were harmed because "Clearview didn't properly inform Illinoisans in writing that their biometric identifiers were being captured and stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers were being captured, stored, and used." Compl. ¶ 71. That alleged harm does not arise from the licensing or advertising

[1] The balance of the Opening Brief relates to Clearview's motion to dismiss pursuant to 735 ILCS 5/2-615. Opening Br. at 10-25.

[2] Plaintiffs claim that the exhibits attached to their Opposition demonstrate that Clearview "directly market[ed]" in Illinois. Opp'n Br. at 8. However, the majority of the exhibits are automated emails or customer service e-mails Clearview sent to people who were *already* licensed users of Clearview's product. Those materials simply do not constitute "marketing."

of Clearview's search engine to third parties. In fact, the alleged collection without consent occurred *before* any of the conduct that Plaintiffs allege subjects Clearview to jurisdiction—and it occurred outside of Illinois. "[I]t could hardly be said that the injury at issue here 'arose out of' contacts that were . . . after the fact." *Tile Unlimited, Inc. v. Blanke Corp.*, 47 F. Supp. 3d 750, 767 (N.D. Ill. 2014) (no personal jurisdiction over defendant whose 2012 contact with Illinois had "no relation to [defendant]'s contacts with Illinois at the time of this suit" or earlier).

That some of the photographs collected by Clearview were allegedly of Illinoisans also cannot give rise to jurisdiction. "The inquiry whether a forum State may assert specific jurisdiction over a nonresident defendant 'focuses on the relationship among the defendant, the forum, and the litigation' . . . [and] the relationship must arise out of contacts that the 'defendant *himself*' creates with the forum State.'" *Walden v. Fiore*, 571 U.S. 277, 283-84 (2014) (emphasis in original). However, the relevant inquiry is on a defendant's conduct, not the location of the plaintiff or where the plaintiff was allegedly damaged. *J.S.T. Corp. v. Foxconn Interconnect Tech. Ltd.*, 965 F.3d 571, 578 (7th Cir. 2020). Here, Plaintiffs do not allege that Clearview collected any photos while in Illinois or that Illinois was the "focal point" of the collection effort, as would be necessary to give rise to jurisdiction. *Calder v. Jones*, 465 U.S. 783, 789 (1984).

Plaintiffs primarily rely on *Russell v. SNFA*, 2013 IL 113909, but *Russell* supports Clearview. Opp'n Br. at 6. In *Russell*, the plaintiff sought damages from a French manufacturer of custom bearings after a helicopter using one of the parts was involved in a fatal crash in Illinois. The *Russell* court held that jurisdiction was proper under a "stream-of-commerce" theory because the foreign defendant "knowingly used a distributor" who sold the defendant's helicopter "products in Illinois," and the foreign defendant itself had a "business relationship" with an Illinois company "for defendant's custom-made bearings used in airplanes." 2013 IL 113909, ¶¶ 11,

78-79, 85. Thus, the defendant's contacts with Illinois directly gave rise to the harm.

Unlike in *Russell*, Plaintiffs here do not allege that the injuries to their members occurred *because* Clearview marketed or sold its product in Illinois. Rather, Plaintiffs allege that their harm arose when Clearview collected their information on the Internet, which Plaintiffs make no effort to connect to Clearview's marketing and sales. Plaintiffs try to avoid this conclusion by arguing for a "course of conduct" theory, claiming that jurisdiction is proper based on "Clearview's capture of Illinoisans' faceprints, consolidation of those faceprints in a massive database, and offer of that database for sale to Illinois entities." Opp'n Br. at 6. However, Plaintiffs cite no authority for their novel theory, which ignores the Supreme Court's requirement that courts may look only at the "very activity" out of which the "cause of action arises"—not the party's entire "course of conduct." *Keeton*, 465 U.S. at 780.

Plaintiffs' attempt to distinguish the most analogous case, *Gullen v. Facebook*, No. 15 C 7681, 2016 U.S. Dist. LEXIS 6958 (N.D. Ill. Jan. 21, 2016), also fails. Plaintiffs claim *Gullen* is distinguishable because the "court held that there was 'no relationship' between Facebook's general sales and marketing activities in Illinois, and its face recognition technology." Opp'n Br. at 7 (quoting *Gullen*, 2016 U.S. Dist. LEXIS 6958). But that is precisely the situation here. Just as in *Gullen*, Clearview's "sales and advertising" activities in Illinois have "no relationship to this suit, which arises from [Clearview]'s alleged collection of biometric data from a photo, not from its sales, marketing, or other business activity in Illinois." 2016 U.S. Dist. LEXIS 6958, at *5. Plaintiffs also try to distinguish *Gullen* by arguing that "Clearview's faceprint database is the very product being marketed and sold in Illinois," Opp'n Br. at 7; however, Facebook also marketed and sold its product in Illinois, which included a "face database," 2016 U.S. Dist. LEXIS 6958, at *2; *see also Bray v. Lathem Time Co.*, No. 19-3157, 2020 U.S. Dist. LEXIS 53419, at *10 (C.D.

Ill. Mar. 27, 2020) (finding no specific jurisdiction because "[t]his lawsuit concerns [defendant]'s alleged collection, storage, use and disclosure of biometrics—not [defendant]'s sales" and marketing activities). Because the alleged injury that Plaintiffs have identified is unrelated to Clearview's alleged contacts in Illinois, Plaintiff cannot show that their claim "arises" from Clearview's activities in Illinois, as is required to adequately allege jurisdiction.

II. BIPA Does Not Regulate Out-Of-State Conduct

A. The BIPA Claim Violates the Extraterritoriality Doctrine

The parties agree that BIPA does not have exterritorial effect. Opp'n Br. at 10. Plaintiffs do not dispute that, to state a claim, they must show that "the *majority* of circumstances relating to the alleged violation" of BIPA occurred in Illinois. *Landau v. CNA Fin. Corp.*, 381 Ill. App. 3d 61, 65 (1st Dist. 2008) (emphasis added). Plaintiffs' BIPA claim fails because Plaintiffs cannot meet this standard.

Plaintiffs argue that BIPA applies to Clearview's alleged conduct because "images of Plaintiffs' members on the internet were almost certainly created in and uploaded from Illinois." Opp'n Br. at 10. However, the Illinois Supreme Court has explained that the extraterritoriality analysis is not "based on the residency of the plaintiff." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 182. Plaintiffs' cases on this point are all materially different from the fact pattern here. Opp'n Br. at 10 (citing *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1101-02 (N.D. Ill. 2017); *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547 (N.D. Cal. 2018)). In each of those cases, the plaintiffs' accounts with defendants identified themselves as being in Illinois and plaintiffs uploaded their photos directly to the *defendant's product*. Opening Br. at 13. That is not the case here. Plaintiffs allege that their members' photos were uploaded to the Internet—specifically, the websites of third parties such as Facebook, YouTube, and Twitter. Compl. ¶ 44. Plaintiffs do not (and cannot) allege that photos were uploaded in Illinois to

Clearview's product. In fact, Plaintiffs do not allege they have had any contact with Clearview whatsoever.

Plaintiffs also mischaracterize Clearview's argument, claiming that "Clearview suggests that because it uses servers outside of Illinois, BIPA cannot apply to it." Opp'n Br. at 11. However, Clearview argues that the location of Clearview's servers is but one of several relevant facts that, when taken together, demonstrate that its conduct at issue did not occur in Illinois. *See* Opening Br. at 12. More significantly, Plaintiffs do not allege that Clearview captured any images from Illinois or that Clearview scanned any images in Illinois. Thus, the very facts giving rise to Plaintiffs' BIPA claim—*i.e.*, the alleged "capturing, storing, and using" of biometric information, Compl. ¶ 73—did not occur in Illinois.

Finally, Plaintiffs' argument that "extraterritoriality is an issue better decided on a fully developed record," Opp'n Br. at 12, ignores the cases cited by Clearview granting motions to dismiss on extraterritoriality grounds, where, as here, the Complaint fails to allege that the relevant facts occurred "primarily and substantially" in Illinois. Opening Br. at 11-12 (citing cases). Because of that omission, the Complaint should be dismissed.

B. Plaintiffs' Application of BIPA Would Violate the Dormant Commerce Clause

Plaintiffs next argue that their application of BIPA does not violate the dormant Commerce Clause because "BIPA does not prohibit the capture of faceprints altogether—it only prohibits such capture without notice and consent from affected Illinoisans." Opp'n Br. at 12. Plaintiffs ignore the realities of the Internet, which does not have geographical boundaries.

Because Illinois residents can travel to, take photos in, and upload photos from other states, and because many photos on the Internet bear no indication of who is in the photo or where they are from, in many instances, Clearview has limited means by which to identify which photos on the Internet are of Illinois residents. If an Illinois resident goes on vacation to New York—a state

that has rejected BIPA-style legislation—takes a photo of herself in front of a New York landmark, and uploads that photo to a social media site while in New York, Clearview likely would have no way of knowing that the photo was of an Illinois resident, and thus no way of knowing it has to offer that person certain information before collecting a photo that is *already publicly available*.[3]

Plaintiffs oversimplify this problem, claiming that all Clearview must do is "comply[] with Illinois law in Illinois and New York law in New York." *Id.* at 13. However, Plaintiffs' own Complaint concedes that it is impossible to determine whether many publicly-available photos have any connection to Illinois. Compl. ¶ 48 ("[A] significant portion of photos of Illinois residents that appear online will not contain geolocation information.").

Plaintiffs' own allegations make plain that under Plaintiffs' application of BIPA, to comply with BIPA, Clearview would either need to (i) provide BIPA disclosures and obtain BIPA consents for all photos on the Internet or (ii) not collect any photographs on the Internet simply because they might relate to someone in Illinois. Plaintiffs' application of BIPA would be a clear burden on interstate commerce. *See Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989) (The dormant Commerce Clause "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State.").

Contrary to Plaintiffs' contentions, the dormant Commerce Clause issue is not "premature." Opp'n Br. at 13. Unlike in *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *15 (N.D. Ill. Sept. 15, 2017), the Complaint facially violates the dormant Commerce Clause because Plaintiffs allege that it is difficult, if not impossible, to determine whether many publicly-available photographs on the Internet are taken in Illinois or are of Illinois

[3] This problem did not exist in *In re Facebook Biometric Info. Privacy Litig.*, No. 3:15-cv-03747, 2018 U.S. Dist. LEXIS 81044, at *14 (N.D. Cal. May 14, 2018) because unlike Clearview, Facebook has a direct relationship with the users who upload photos to its product, which means Facebook can "activate or deactivate features for users in specific states with apparent ease when it wants to do so."

residents. Compl. ¶¶ 48-50. This very impossibility means that the relief sought by Plaintiffs violates the dormant Commerce Clause.

III. Plaintiffs' Claim Is Barred by the First Amendment and Article One Section Four of the Illinois Constitution

Neither the ACLU and its co-plaintiffs nor its two *amici curiae* allies take issue with a significant portion of Clearview's First Amendment argument. None rejects the proposition that Clearview is constitutionally entitled to compare photographs posted on the public Internet with photographs furnished to it by its users to see if they match each other. None disputes that as a matter of established law, individuals depicted in those photographs have no reasonable expectation of privacy. And none denies that Clearview does not know and could not know the names of the multitude of individuals who have posted photographs on the public Internet that have been obtained by it and thus cannot obtain their consent as required by BIPA before it can use its technology.

Significantly, all three briefs submitted in support of Plaintiffs' position urge the Court to subject the application of BIPA to Clearview's services to First Amendment scrutiny—although all three briefs apply different analyses leading to some form of intermediate scrutiny.[4] None of the briefs submitted in support of Plaintiffs even attempt to argue that the First Amendment does not apply here. That is of enormous significance in this case since regardless of what level of First Amendment scrutiny applies, Plaintiffs' claim fails to pass constitutional muster.

A portion of the *amicus curiae* brief in support of Plaintiffs submitted by the Electronic Frontier Foundation ("EFF") offers a useful introduction. It begins its analysis of the nature of the

[4] *See* Opp'n Br. at 14-22 (urging intermediate scrutiny under *United States v. O'Brien* because Clearview is engaged in conduct with "speech elements"); *Amici* Law Professors ("ALP") Br. at 4-10 (urging intermediate scrutiny because BIPA is a content-neutral time, place, and manner restriction); EFF Br. at 2-17 (urging intermediate scrutiny because Clearview engages in commercial speech).

First Amendment protection at issue in this case this way: "The First Amendment protects not just expression, but also the necessary predicates that enable expression, including the collection and creation of information. . . . [H]ere, Clearview uses face printing to sell to its law enforcement clients the service of providing information about an unidentified suspect in a police photo." EFF Br. at 2-3. The brief later states that "faceprinting is both the collection and creation of information. It collects information about the unique shape and measurements of a person's face. And it creates information about that face in the form of a unique representation." *Id.* at 5. While we strongly differ with many assertions and conclusions in EFF's brief, including its argument that BIPA's application to Clearview survives First Amendment scrutiny, we agree with EFF that, under First Amendment principles, Clearview's service triggers First Amendment protection because it collects and creates information designed to communicate to its users useful information about the degree to which individuals in publicly-available photos are the same as individuals in photos uploaded by the users of Clearview's app.

Plaintiffs' brief offers little recognition of the central role the First Amendment plays in our nation. It recognizes neither of the two well-established propositions set forth in EFF's brief (and Clearview's) that the collection and creation of information receives First Amendment protection, as do the predicates to speech that enable that expression. What Plaintiffs' brief *does* say about Clearview's position is simply inaccurate. It sets up a classic "straw person" argument by asserting that Clearview's position is that applying BIPA's notice-and-consent requirement to it prevents Clearview "from republishing publicly-available photographs." Opp'n Br. at 16. That, however, is not Clearview's position at all. What that requirement actually does is to effectively prevent Clearview from *comparing* the public photographs in its possession with photos provided

to it by users in a manner that allows Clearview to determine if there are matches between the two. Plaintiffs do not and cannot deny the accuracy of that reality.[5]

The central First Amendment issue here is not whether BIPA's provisions are ever or even often constitutional. Clearview does not argue that BIPA is facially invalid, but only that the law's application to Clearview's conduct violates the First Amendment since "BIPA restricts, in the name of privacy, Clearview's ability to 'collect, capture, purchase, receive through trade or otherwise obtain,' or 'profit from' the publicly available information Clearview uses in its search engine." Opening Br. at 19-20. *Austin* made indelibly clear that "the Supreme Court has repeatedly reconciled the tension between the right to privacy and free speech by analyzing the specific privacy claim and the public interest in the communication in each case." *People v. Austin*, 2019 IL 123910, ¶ 64. That is precisely what this Court should do.

Plaintiffs' claim is sweepingly broad: in all situations, if a "faceprint" is created it must be destroyed unless the individual portrayed consents to its use. And the First Amendment claim is narrow: in a situation, as here, in which it is impossible to obtain consent from every (usually unidentified) person whose photo is on the public Internet and in Clearview's possession, none of whom, as a matter of law, has any reasonable expectation of privacy, and the purpose of creating and analyzing that person's "faceprint" is to allow users to determine if that person is the same as in another photo, the First Amendment interest should be vindicated.

Clearview's position is that in resolving this case, strict scrutiny should be applied. Plaintiffs and both of their *amici* maintain that intermediate scrutiny is the correct test. The

[5] The brief of the *Amici* Law Professors similarly mischaracterizes Clearview's position. That brief attributes to Clearview the position that BIPA impedes "its ability to collect publicly available photographs," when Clearview's actual position is that it already has publicly-available photographs and that the application of BIPA to it would frustrate or even end its ability to efficiently compare those photographs to ones forwarded to them by their law enforcement clients. *See* ALP Br. at 2.

distinction is particularly important, since neither Plaintiffs nor their *amici* even claim that the application of BIPA to Clearview's conduct can satisfy the demanding strict scrutiny test; one rooted in the proposition that, since content-based regulations are "presumptively unconstitutional," they may be applied only when they are "narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).

Strict scrutiny is applied when a statute is content-based, and BIPA is content-based because it "target[s] speech based on its communicative content." *Id*. As applied to Clearview, that is precisely what BIPA does.

Strict scrutiny also is applied when statutes distinguish between whose speech is subject to a law and whose is not. *See Sorrell*, 564 U.S. at 570-71. That is the case here, because BIPA exempts from its coverage any "contractor, subcontractor, or agent of a State agency," 740 ILCS 14/25(e), making it "speaker-based." Strict scrutiny should also be applied because BIPA imposes limitations on the collection of data that are designed to and do make it difficult to communicate a message that the State of Illinois has deemed harmful and violative of privacy rights—namely, that a publicly-available photo is likely of the same person as a photo uploaded by the users of Clearview's app. Just as the Supreme Court applied "heightened scrutiny" to a statute that had the "purpose and practical effect" of limiting the effectiveness of communicating about data concerning pharmaceutical prescriptions, *Sorrell*, 564 U.S. at 565, so the Court here should apply heightened (i.e., strict) scrutiny to BIPA, which has the "purpose and practical effect" of limiting the effectiveness of Clearview's efforts to communicate about the similarity of data concerning photos of interest to law enforcement.

Strict scrutiny is also applied when, as here, laws effectively bar the dissemination of data.[6] That principle is especially applicable in this case because it is inherently content-based to limit one way of gathering information—through computer-created "faceprints" used within Clearview's service—while permitting virtually all others (e.g., use of workers with photographic memories to match photos with other photos on the Internet).

As we observed earlier, Plaintiffs make no effort even to argue that the application of BIPA to Clearview could withstand strict scrutiny. Nor can such application withstand the more relaxed intermediate scrutiny standard. BIPA's application here is not limited in scope to some sort of misuse of "faceprints" but to *all* "faceprints"—even, as in this case, when they are used only within search engines as part of an effort to identify potential criminals.

As phrased by Plaintiffs, BIPA "broadly proscribes nonconsensual faceprinting, without respect to how the faceprints may ultimately be used." Opp'n Br. at 21. But that is not a defense of the statute; it is a confession of its overbreadth and therefore its unconstitutionality. If "faceprints" are used only within a search engine to assist in determining if an individual in one photograph is the same as one in another, there is no state interest at all that can justify all but banning doing so. As applied to Clearview, the statute therefore can hardly be defended, as Plaintiffs contend, as imposing restrictions that are "no greater than is essential to the furtherance of" a substantial government interest. *Id.* at 18. That is, as Plaintiffs and their *amici* concede, a requirement for any statute to be held constitutional when intermediate scrutiny is applied. *Id.* at 18, 21; ALP Br. at 9-10; EFF Br. at 12-17. The overbreadth of BIPA—its alleged application to a situation as in this case, where a "faceprint" is simply created as an intermediate step for use in a

[6] *See* A. Bhagwat, "*Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy," 36 Vt. L. Rev. 855, 867 (2012) ("[F]or a restriction on the disclosure of data to survive a constitutional challenge, it must survive strict scrutiny.").

search engine to determine who is in a public photograph—is also an independent basis for granting the motion to dismiss. *See* Opening Br. at 22-23.

In the First Amendment arena, narrowness in drafting statutes is essential. *People v. Sequoia Books, Inc.*, 127 Ill. 2d 271, 288 (1989) (recognizing that "regulation of any form of expression, even of obscenity, [must] be carefully drawn so as not to impact unduly upon protected speech"); *People v. Burkhardt*, 11 Ill.App.3d 760, 765 (1st Dist. 1973) ("[T]he danger of a violation of cherished First Amendment rights necessitates [a] narrow construction.") (citation omitted).

That it is undisputed here that the photos at issue are publicly available and that courts have repeatedly held that individuals have no valid privacy interest in such materials further exacerbates the challenge to Plaintiffs in defending the statute. To satisfy intermediate scrutiny, Plaintiffs have the burden of affirmatively demonstrating that the harms to be addressed by BIPA in this context "are real" and that the restriction on speech "will in fact alleviate them to a material degree." *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993). This burden cannot be satisfied by mere speculation or conjecture. *Id.* at 771. And in this case, it cannot be established at all.

Applying BIPA to an entity such as Clearview, which does not use faceprints for any purpose other than comparing one set of public photographs to ones provided by users, serves no public purpose at all and cannot withstand any First Amendment scrutiny.

IV. BIPA Does Not Apply to Clearview's Use of Photographs

Clearview's argument regarding BIPA's photo exemption is straightforward and textual. BIPA's definition of "biometric identifier" excludes "photographs," and its definition of "biometric information" excludes "information derived from items or procedures excluded under the definition of biometric identifiers," such as photographs. 740 ILCS 14/10. As a result,

information obtained from photos is not covered by BIPA.

In response, Plaintiffs argue that the plain language of BIPA does not mean what it says. Specifically, Plaintiffs argue that BIPA's definition of "biometric identifier" "says nothing about *how* these identifiers are collected," and Plaintiffs therefore conclude that this must mean that biometric data can be collected from photographs. Opp'n at 24. BIPA's requirement of informed consent at the time of collection, however, demonstrates the legislature's intent that the collection of biometric identifiers would occur in person, permitting the collector the opportunity to obtain the required consent. Opening Br. at 24-25. Any other reading "would produce an absurd and unjust result" because it would often be impossible to comply with this provision. *Clinton v. City of New York*, 524 U.S. 417, 429 (1998). The Court should not adopt an interpretation of BIPA that ignores the plain language of the statute.

CONCLUSION

For these reasons, Clearview respectfully requests that the Court dismiss the Complaint.

DATED: November 23, 2020 JENNER & BLOCK LLP

By: *s/ Lee Wolosky*

Lee Wolosky (pro hac vice)
Andrew J. Lichtman (pro hac vice)
JENNER & BLOCK LLP
919 Third Avenue
New York, New York 10022-3908
Phone: (212) 891-1600
lwolosky@jenner.com
alichtman@jenner.com

David P. Saunders
Howard S. Suskin
JENNER & BLOCK LLP
353 North Clark Street
Chicago, Illinois 60654
Phone: (312) 222-9350
hsuskin@jenner.com
dsaunders@jenner.com

Floyd Abrams (pro hac vice pending)
Joel Kurtzberg (pro hac vice pending)
CAHILL GORDON & REINDEL LLP
32 Old Slip
New York, NY 10005
Phone: (212) 701-3000
fabrams@cahill.com
jkurtzberg@cahill.com

Attorneys for Defendant Clearview AI, Inc.

CERTIFICATE OF SERVICE

I, David Saunders, an attorney, hereby certify that I caused a copy of the foregoing Reply Memorandum of Law to be served on all counsel of record via email on this 23rd day of November 2020.

Jay Edelson
jedelson@edelson.com
Benjamin H. Richman
brichman@edelson.com
David I. Mindell
dmindell@edelson.com
J. Eli Wade-Scott
ewadescott@edelson.com
Edelson PC
350 North LaSalle Street, 14th Floor
Chicago, IL 60654
3120589-6370

Rebecca K. Glenberg
rglenberg@aclu-il.org
Karen Sheley
ksheley@aclu-il.org
Juan Caballero
jcaballero@aclu-il.org
Roger Baldwin Foundation of ACLU, Inc.
180 North Michigan Avenue, Suite 2300
Chicago, Illinois 60601
Tel: 312.201.9740

Nathan Freed Wessler
nwessler@aclu.org
Vera Eidelman
veidelman@aclu.org
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500

Adam Schwartz
adam@eff.org
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
415-436-9333

Craig Futterman
futterman@uchicago.edu
Mandel Legal Aid Clinic
University of Chicago Law School
6020 S. University Ave.
Chicago, IL 60637
773-702-9611

By: /s/ *David P. Saunders*
David P. Saunders